Secure Key Management for NASA Space Communication

A. Balasubramanian[1], S. Mishra[1], R. Sridhar[2]

[1]CompSys Technologies Inc., Amherst, NY

[2]Department of Computer Science and Engineering,
University at Buffalo (SUNY), Buffalo, NY

Overview

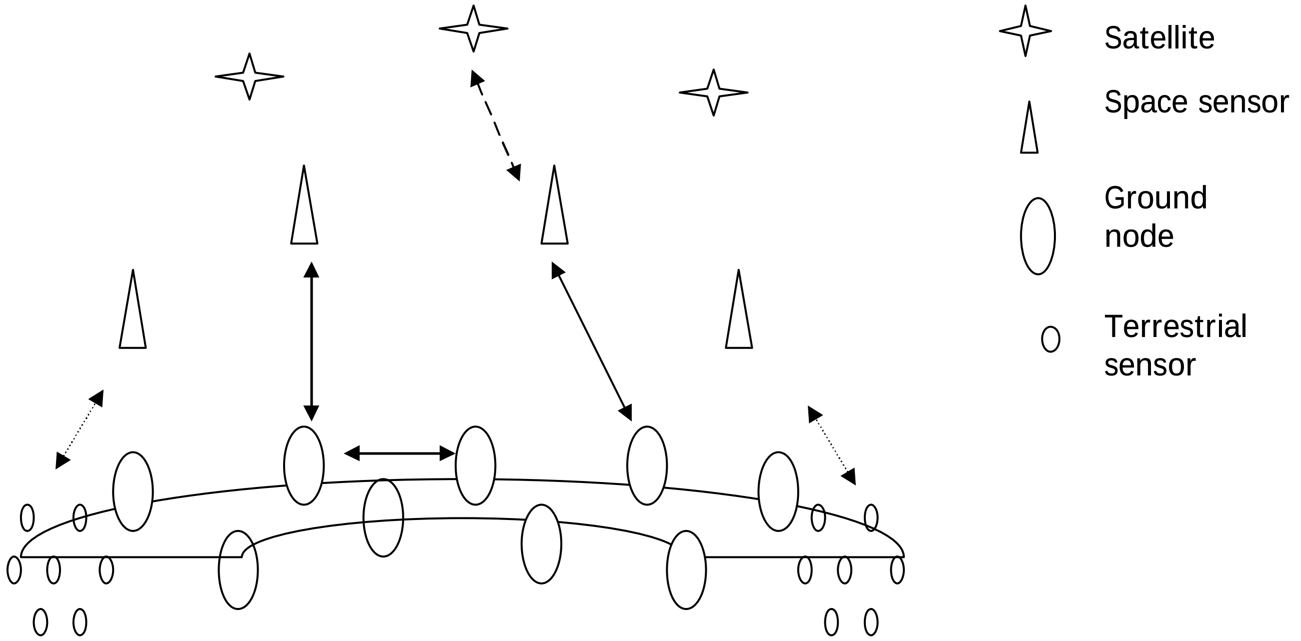
- Space based networks
  - Architecture
  - Security
- State of the art
- Proposed security solution
  - Classification of space-based networks
  - Security solutions suitable for the classifications
- Conclusions and Future work
- References

Space Based Networks

- All nodes (space and terrestrial) are part of one large network
- Satellite communication is no longer just point to point
  - A satellite can contact any terrestrial node to relay information to its ground controller
  - Cost effective
  - Smaller delays
- Examples
  - Myriad of loosely coupled ground stations
  - Sensor webs

Space Based Networks: Architecture

- Components of space-based networks considered here
  - Satellites, Space sensors, Ground nodes, Terrestrial sensors



Space Based Networks: Security

- Traditional NASA security solution
  - Security through obscurity
- Security risks introduced by space-based networks
  - Space network is no longer obscure
  - Easier to compromise the protected space network by compromising the relatively insecure ground network
- Challenges in providing a security solution
  - Space networks are heterogeneous
  - Network components vary in security requirement and resource limitations
  - A generic security solution catering to all space based network component may not always be efficient

State of the Art

- Communication protocol for space-based networks
  - SCPS (Space Communication Protocol Specification) is used for space communication
  - IP (Internet Protocol) is used for ground communication
  - CCSDS (Consultative Committee for space data systems) developed SCPS-Security Protocol for securing space communication
  - IPSec is used to secure ground communication
- OMNI (Operating Missions as Nodes in the Internet)
  - IP is used for all communication and IPSec is implemented for security
- Security is implemented in layer-3

State of the Art: IPSec and SCPS-SP

- SCPS-SP is a bit optimized version of IPSec
- Source and Destination share a secret key and create a security association (SA)
- SA determines parameters such as the length of the key and the encryption algorithm
- All layer-3 packets exchanged between the source and destination are encrypted
- Internet Key Exchange Protocol (IKE)
  - used for key management, to implement IPSec or SCPS-SP
  - consists of OAKLEY (for key exchange) and ISAKMP (for establishing SA)
  - uses pair-wise algorithms

Security Solution: Overview

- Need for a security solution
  - Pair-wise communication introduces high overheads
  - The operational IKE reduces bandwidth utilization to an extent, but may not provide strong authentication
  - Heterogeneous networks have different security requirements and constraints
- Proposed solution
  - Classifies network components in terms of their characteristics
  - Provides a suitable security solution based on the classification
  - The solution is layer and architecture independent

Security Solution: Classification

- Parameters used for classification
    - Resource constraint
    - Mobility
    - Data rate of communication

	Resource Constraint	**Mobility**	**Data rate of communication**
Terrestrial sensors	High (Computational)	Low	Low
Space sensors	Low	High	High
Ground node	Low	Low/Medium	High
Satellite	High (Bandwidth)	Medium	Low

Security Solution: Classification

- Three communication sub-networks are considered in this work
- Intra-Ground
  - High data rate of communication
  - Typically low resource constraints
  - May need a decentralized solution
- Satellite – Space sensor
  - Low rate of communication
  - Have bandwidth constraints
- Space sensor – Terrestrial sensor
  - Low rate of communication
  - Constrained in terms of computational resources

Security Solution: Intra-ground

- Security for ground nodes is very critical
  - Compromising a ground node may lead to a compromise of the protected space network
  - Attacks on the ground network is relatively easier
- Any ground node can be designated as a receiving station
  - Thus, connectivity to a central server may not be always feasible
- We propose a symmetric/asymmetric key based hybrid key management solution that is
  - Decentralized, scalable and low cost
  - Secure against insider and outsider attacks
  - Suitable for wired and wireless networks

Security Solution: Intra-ground

Hybrid Security Solution: Overview

- Symmetric keys
  - Pair-wise keys exchanged between every pair of nodes
  - Not scalable, computationally inexpensive
- Asymmetric keys
  - One pair of (public, private) key for every node
  - Scalable, computationally expensive
- Hybrid
  - Locally symmetric, globally asymmetric
  - Restricting symmetric keys to local communication ensures scalability
  - Reduced use of asymmetric encryption decreases cost

Security Solution: Intra-ground

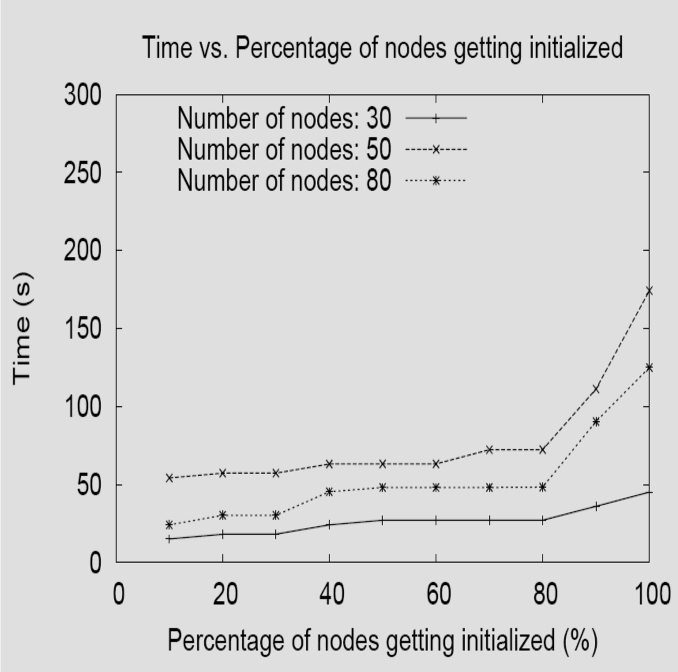
Hybrid Security Solution: Algorithm

- Divide nodes into non-overlapping clusters
- Create group key for cluster nodes
- We have developed a novel algorithm to determine symmetric and asymmetric keys from the group key
  - Symmetric keys are computed by nodes themselves
  - No need for explicit key exchange
  - Symmetric keys are used to encrypt intra-cluster communication
  - Asymmetric key are used to encrypt inter-cluster communication

Security Solution: Intra-ground

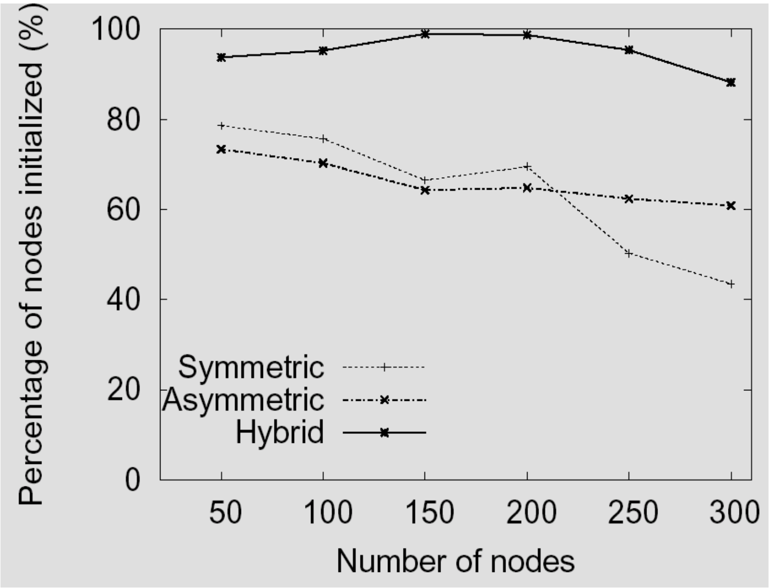
Hybrid Security Solution: Results

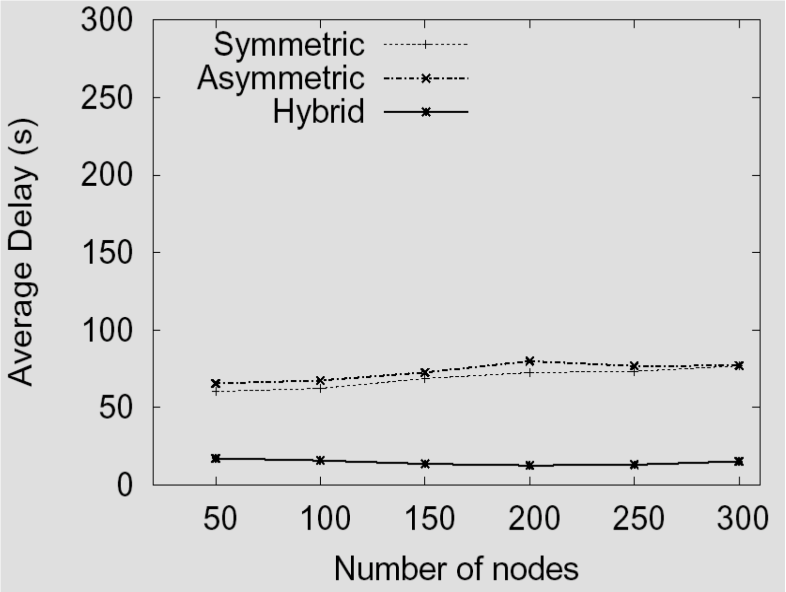
- Current simulation using a network simulator called GloMoSim
- Metrics used are
  - The percentage of nodes getting successfully initialized.
  - Delay in initialization
- Initialization is a state when nodes receive keys for secure communication



Security Solution: Intra-ground

Hybrid Security Solution: Results





Security Solution: Satellite – Space sensor

- Satellite – Space sensor characteristics
  - Bandwidth constraints
  - Satellites are statically keyed. No key management necessary
- However, in space-based networks, satellites contact several ground stations
- A satellite sharing the same secret key with all ground nodes may not be always feasible
- Increased network activity decreases key lifetime and increases the need for re-keying
- We propose an efficient key management protocol for re-keying, in a bandwidth constrained network

Security Solution: Satellite – Space sensor

- During its orbit, a satellite can communicate with a space sensor with which the

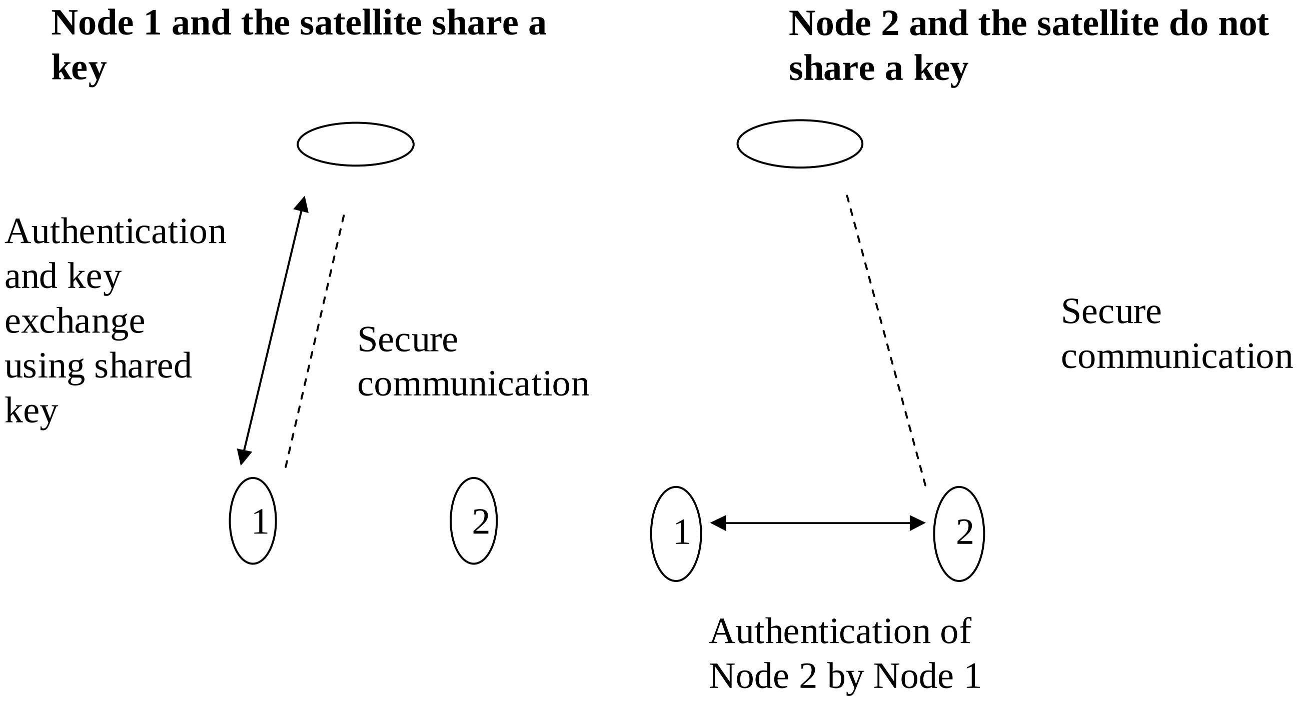
  1) satellite shares a key

  2) satellite does not share a key

  3) satellite shares a key, but the key needs to be refreshed

- For cases 2 and 3,
  - Authentication and key exchange is implemented among the space sensor
  - Secret key that is generated in the previous step is distributed to the satellite
  - Developing a low cost algorithm for this distribution, using a novel and cryptographically secure Pseudo Random Number Generator

Security Solution: Satellite – Space sensor


Node 1 and the satellite share a key

Authentication and key exchange using shared key

Secure communication

Node 2 and the satellite do not share a key

Secure communication

Authentication of Node 2 by Node 1

Security Solution: Terrestrial sensor– Space sensor

- Work in Progress
- Characteristics: Low rate of communication, low computational resources
- Assume that terrestrial sensors are statically keyed and use only one key to communicate with all space sensors
- Solution
  - Using keys of small length to provide prolonged security
  - Efficient key refresh algorithm
  - Algorithm to communicate the refreshed key to the terrestrial sensor and all the space sensors that share a key with it

Conclusions and Future Work

- Analyzed the security risks for a space based network architecture
- Classified the space-based network components based on certain identified parameters
- Using the classification, analyzed three sub networks formed among one or more network components
- Provided suitable key management solutions for the sub networks
- Future work: Study the feasibility and performance of the proposed solution via simulation and analysis
- Future work: Extend the framework to provide solutions for other space-based network architectures

References

1) William Ivancic, "*Architecture study of space-based satellite network for NASA missions",* IEEE Aerospace Conference, Montana, March 2003.

2) Space Communication Protocol Specification (SCPS) – CCSDS 713-5-B-1, CCSDS, May 1999

3) J. Noles, K. Scott, M.J. Kukoski and H.Weiss, *"Next Generation Space Internet",* 2nd ESA Workshop on Tracking Telemetry and Command Systems for Space Applications, 2001.

4) A. Balasubramanian, S.Mishra and R.Sridhar, "*Analysis of a Hybrid Key Management Solution for MANETs",* IEEE Wireless Communication and Networking Conference, New Orleans, LA, March, 2005.